Every transistor has a unique quantum fingerprint—but can it be used as a form of ID?

29 July 2019, by Lisa Zyga

Single-electron effects in transistors can lead to unique electric properties that could be used for security purposes. Image credit: Pixabay

We might imagine that electric current flows as a smooth, even stream of electrons through our electronics devices, but at the quantum scale the flow of electric current might be more accurately pictured as a bubbling brook containing many tiny ripples. These ripples can be caused by single-electron effects, which arise due to the repulsion among electrons confined in very small spaces, such as trap sites in transistors. Single-electron effects can lead to tiny changes in the current-voltage characteristics of these devices.

As trap sites are basically tiny defects that are randomly distributed in an uncontrollable way during fabrication, the number, location, and energy levels of trap sites differ for every transistor. As a result, single-electron effects lead to a unique modification in the current-voltage characteristics, effectively giving each transistor a unique "fingerprint."

Recently, researchers have been investigating how these quantum fingerprints might one day be used as an inexpensive form of ID to protect users' personal information for technologies in the emerging network of internet-connected devices known as the Internet of Things.

In a new paper published in *Applied Physics Letters*, physicists T. Tanamoto and Y. Nishi at the Toshiba Corporation in Kawasaki, Japan, and K. Ono at RIKEN in Saitama, Japan, have demonstrated that single-electron effects may be detected by image-recognition algorithms and used for computer chip identification and security.

"So far, no widespread application exists for single-electron devices," Tanamoto told *Phys.org*. "Our research opens a different way of using the single-electron effect: as a security device. The importance of security is increasing day by day."

As the physicists explain, the fingerprint of an electronic device can be thought of as a physically unclonable function (PUF). Like a human fingerprint, PUFs are based on unique, naturally occurring physical variations and cannot be transferred to other devices. In addition, PUFs retain their key features throughout the lifetime of the device, despite some degradation due to aging effects.

In their work, the physicists applied image-matching algorithms in order to identify different current-voltage features called Coulomb diamonds. The Coulomb diamonds are so-named because the regions of a current-voltage diagram in which current is suppressed by single-electron effects sometimes have the shape of a diamond. As the number of trap sites increases, the diamond patterns because more complex.

Just as human fingerprints change depending on

conditions, such as being wet, dry, or oily, the Coulomb diamond images can also look slightly different when measured under different conditions. Despite these variations, the researchers demonstrated that currently available feature detection and image-matching algorithms could successfully extract the key features (such as corners and edges) and distinguish between different Coulomb diamonds.

One of the advantages of the method is that, although an average computer chip today contains more than a billion transistors, just a single transistor is needed to generate the fingerprint for the entire chip. This makes it potentially feasible to use this method for practical devices, since only one transistor needs to be measured.

On the other hand, there are still challenges that remain before implementing the method. For one thing, the Coulomb diamonds here were measured at cryogenic temperatures of around 1.5 degrees above absolute zero. Previous research has shown that it's possible to measure single-electron effects at room temperature, but currently this ability requires expensive fabrication processes.

In the future, the physicists plan to explore other ways of fingerprinting transistors. One possibility is to measure the spin-qubit behaviors of electrons in traps, as these quantum behaviors are expected to be affected by the traps. As with single-electron effects, the unique and random distribution of traps in transistors is expected to result in a unique fingerprint for each transistor. Going forward, the researchers would also like to investigate ways to implement transistor fingerprint security into future quantum computers.

"Quantum computers are one of the hottest issues right now," Tanamoto said. "We would like to combine our quantum PUF into the security system of quantum computers in the future."

More information: T. Tanamoto, Y. Nishi, and K. Ono. "Application of single-electron effects to fingerprints of chips using image recognition algorithms." *Applied Physics Letters*. DOI: 10.1063/1.5100644